Response to the American Health Information Community
Confidentiality, Privacy, and Security Work Group
Request for Public Input
May 2007

For the past several months, the CPS workgroup has been refining the following "working hypothesis" as an approach to gather information and develop recommendations regarding the protections that should apply to certain persons and entities in a nationwide health information exchange environment. The main tenet of the "working hypothesis" is as follows: *All persons and entities excluding consumers that participate in an electronic health information exchange network at a local, state, regional or nationwide level, through which individually identifiable electronic health information is stored, compiled, transmitted, or accessed, should be required to meet privacy and security criteria at least equivalent to relevant Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule requirements*. In this case, HIPAA is used to help establish a common understanding of what federal health information privacy and security requirements apply to whom and for what. Its inclusion in the "working hypothesis" should not be misinterpreted to mean that the CPS workgroup is only considering HIPAA-focused recommendations. Rather, the CPS workgroup intends to evaluate, in the future, whether the overall, baseline standard for participating in these networks should be changed to a standard that is different from or exceeds the current HIPAA privacy and security rules. The CPS workgroup is interested to hear from any party that may be affected by its "working hypothesis."

1. Enforceable mechanisms

The CPS workgroup understands that there may be one or more appropriate mechanisms to properly enforce and ensure that confidentiality, privacy, and security requirements are met in an electronic health information exchange environment. Therefore, the workgroup is interested in comments on appropriate, effective, and feasible ways to enforce confidentiality, privacy, and security protections in this new environment. Comments will be considered by the workgroup for the purposes of developing one or more recommendations associated with the "working hypothesis" above.

Response: The question presupposes that the current enforcement mechanisms are adequate to protect patient rights and privacy. In general, existing enforcement mechanisms should be the foundation for enforcement at the state and national level and these mechanisms should be strengthened. One possibility is to establish or designate a State-level organization to enforce security within the network of each State on behalf of the NHIN.

2. Relevant requirements

For a given participant's characteristics and role in an electronic health information environment, certain confidentiality, privacy, and security requirements may be more relevant than others. The CPS workgroup requests comment as to whether particular confidentiality, privacy, and security requirements equivalent to those in the HIPAA Privacy and Security Rules should or should not apply to a particular type of person or entity and why. Please identity specific section(s) of the HIPAA Privacy and Security Rules. The following examples have been developed to identify the level of detail and specificity the workgroup is seeking in a response:

> Example 1: Similar to the treatment of health care clearinghouses under the HIPAA Privacy Rule it may not be appropriate for a health information exchange organization to provide privacy notices (Section 164.500 (b)).
>
> Example 2: With respect to Section 164.510 of the HIPAA Privacy Rule, a health information exchange organization may not have a function analogous to a "facility

directory" and therefore compliance with that type of requirement may not be appropriate.

Response: HIPAA is not problematic for health information exchange in patient care. We urge caution in making changes to HIPAA. Please review and incorporate lessons learned from RTI Project and input from the State Alliance. The findings from the RTI project indicate that the most important barriers to health information exchange is confusion about HIPAA requirements and other federal and state laws that are inconsistent with HIPAA.

3. Business Associates

The CPS workgroup is concerned that an electronic health information exchange environment may lead to an unwieldy amount of contractual relationships in the form of business associate agreements each with their own specific confidentiality, privacy, and security nuances – with limited direct enforcement. The workgroup is seeking comments on the pros and cons of having business associates directly responsible for HIPAA requirements – not through contractual arrangements. **If you are a business associate please answer the following questions**:

A) How does you organization ensure compliance with the privacy and security policies of covered entities with whom it contracts, particularly when there are numerous contracts?
B) How do you handle business associate contracts with large numbers of covered entities including compliance with each covered entity's privacy policies?
C) How are business associate agreements negotiated? Do you have a standard contract?
D) How is the data protection compliance of subcontractors ensured and/or assessed?
E) Do you have subcontractors and how do you handle those agreements?
F) How would direct accountability for meeting relevant HIPAA requirements impact your business?

Response: Health information exchanges including paper-based exchanges require trust relationships but there needs to be a level playing field regarding accountability and enforcement to the extent possible. Expanding direct accountability for meeting relevant HIPAA requirements to those entities routinely handling protected health information such as personal health records systems would probably be beneficial.

4. General Questions

The CPS workgroup is seeking comment on any of the following additional questions.

A) What are the implications of having some entities performing similar services covered by federal law (e.g., HIPAA) and others not? For example, a personal health record (PHR) could be offered by a health plan (covered entity) and an independent PHR service provider (non-covered entity).
    i. How does this impact your competitiveness?
    ii. How does this impact your ability to exchange information with others?
    iii. Does contracting with non-covered entities create different levels of accountability and/or enforceability in the exchange of health information?
B) **Assuming you are not a covered entity**, what would be the implications of complying with enforceable confidentiality, privacy, and security requirements at least equivalent to relevant HIPAA principles?
C) Is there a minimum set of confidentiality, privacy, and security protections that you think everyone should follow, if not HIPAA, what?

Yes. HIPAA is the appropriate minimum.